Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 7, pp. 1911–1924
DOI : 10.47974/JDMSC-1725

Performance evaluation of LSB steganography based on multiple image formats

Urmila Pilania *
Manoj Kumar †
Vivaan Mittal §
Department of Computer Sciences & Technology
Manav Rachna University
Faridabad
Haryana
India

Abstract

In the proposed research work steganography technique has been designed and developed for carrier images having different formats. The algorithm is applicable for the image formats: PNG (Portable Network Graphics), TIFF (Tagged Image File Format), JPEG (Joint Photograph Expert Group), and BMP (Bitmap). A single algorithm for almost all types of image formats provides many advantages. Depending upon the size of the secret message, network bandwidth, and allowable distortion we can choose the format of the carrier. For embedding secret messages, the LSB substitution technique is applied in this paper. We utilized the concept of imperceptibility by calculating PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), SSIM (Structure Similarity Index Metrics), Histogram, and Entropy. The proposed work is analyzed for robustness with favorable results. Two steganalysis tools: Stegexpose and Stegdetect are used to detect the hidden secret message. For analyzing the complexity of work capacity, concealing and retrieval times are calculated. Furthermore, the comparative outcome for the proposed work is very promising for different carrier image formats.

Subject Classification: *Primary 94A08, Secondary 49K15.*

Keywords: *Image steganography, Least significant bit, Steganalysis tools, Robustness, Imperceptibility, Complexity.*

* *E-mail:* **urmilapilania@gmail.com (Corresponding Author)**
† *E-mail:* **manojattri003@gmail.com**
§ *E-mail:* **vivaanmittal2002@gmail.com**

1. Introduction

Multimedia data is now a pretense alarming issue for developers of content, aggregators, distributors, and intermediate users. At this time, we need to design more robust techniques for data processing and storing. Robust techniques can avoid data modification, retrieval of confidential data, and its destruction as well [4]. Cryptography has been used for many years for the security of confidential data. Many techniques can be used to encrypt and decrypt confidential data. Sometimes the safety of secret messages is not enough it is more appreciable if we can hide even the presence of the secret information. The process of hiding the presence of secret data is known as steganography. It is there for thousands of years. It is applied in different forms from time to time classical to digital steganography.

Depending upon the domain in which secret information is hidden, steganography methods are again categorized into spatial domain and transform domain. Spatial domain techniques include LSB (Least Significant Bit), MSB (Most Significant Bit), PVD (Pixel Value Differencing), Pixel indicator, and many more. Spatial domain techniques are simple to conceal the secret message. These techniques modify the pixel values of the carrier file by the pixels of the secret data. These techniques have high embedding capacity and good graphic excellence of the stego file. These techniques are robust against steganalysis techniques or steganalysis tools [7]. Figure 1 represents the categorization of steganography substitution techniques based on different file formats.

In this paper, the LSB image steganography technique is proposed to hide the secret message. The working of the LSB technique is shown in

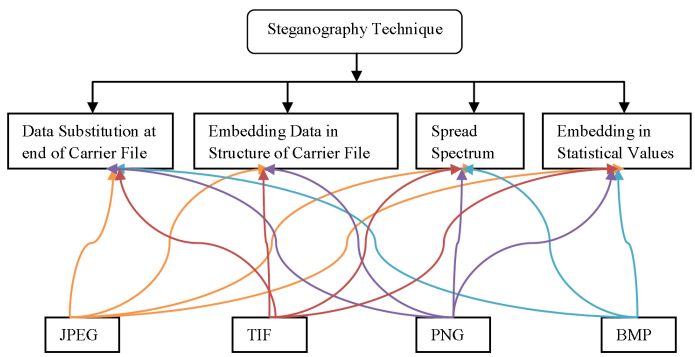


Figure 1

Steganography in Different File Formats

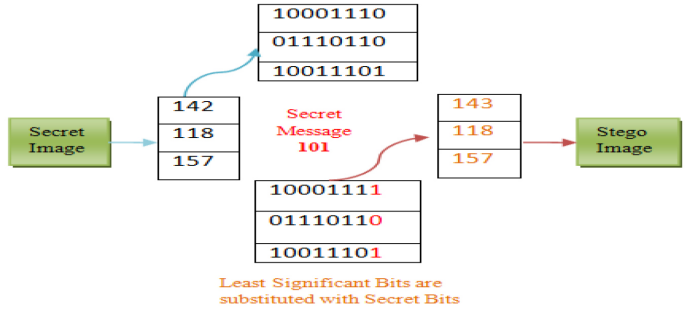


Figure 2

LSB Substitution

Figure 2. Carrier image is taken in different formats such as JPEG, BMP, PNG, and TIF. We designed a general algorithm that can hide secret information in images having different formats mentioned above. Depending upon the type of transporter file steganography can be categorized into text, image, audio, and video steganography. These days image steganography is getting more attention related to other types of steganography techniques. It is also popular due to the wide use of images on the web.

The organization of the proposed work is done in 5 sections. In section 1 we have provided the introduction of the proposed work. Section 2 presents the literature review of the techniques from the same domain. After the literature review, we have also listed various challenges which still exist. Section 3 describes the research design and methodology of the work to overcome some of the existing challenges. Section 4 is devoted to the result analysis and discussion. Section 5 concludes the research work along with its future scopes.

2. Literature Review

Steganography is the procedure of whacking a secret message in a carrier. In the proposed research work DC coefficients were used to conceal the secret message using LSBs. The middle frequency of DC coefficients is used to embed the secret message. As the middle frequency has a high embedding size and better visual quality. PSNR and MSE were used to check the quality of the proposed work. It has been determined that the work has good visual quality and high embedding capacity [1]. In continuation of the previous work, in this research work, an image steganography technique based on the different formats of carrier images

has been proposed. This paper aimed to communicate the secret data from the source to a defined recipient so that no one other than the intended recipient is aware of the secret message's existence. The comparative analysis also has been done in this paper based on carrier file formats. The application of the work also has been done in the proposed work [2].As technology is rising day by day so lots of secret data is being transmitted daily. As many skilled hacks are also there on the web to steal or modify secret data. To avoid editing or stealing secret data we need some techniques which can be used for security purposes. So, to secure secret data authors of this paper used the LSB technique. LSB techniques are simple to use and carry high concealing capacity. In this paper, the author used different file formats to secure the secret data. For the analysis purpose, they calculated values of different evaluation parameters. The proposed work performed well in terms of embedding capacity and imperceptibility [5]. In this paper, the author worked on the tradeoff of the steganography technique. LSB steganography has been proposed by the authors to find an appropriate balance between capacity, imperceptibility, and robustness. Different formats of images have been selected to entrench the secret data. Evaluation of proposed work has been done based on performance metrics such as PSNR, MSE, SSIM, and CC [6].

Extending the concept of the steganography technique author of this paper worked to find whether a single algorithm was able to embed secret data into different formats of images. As all the formats have a different set of rules and color-coding schemes so it was very difficult to apply a single steganography technique. The proposed research work just provides an overview of the existing steganography techniques concerning different formats of images [8]. The image steganography technique is gaining consideration every day. In the proposed work comparative study of different image steganography techniques has been done in the spatial domain. Each technique has its own merits and demerits. Some techniques were carried high embedding capacity but on the other hand not able to resist attacks and vice versa [9].Data transmission on the web is facing problems such as security, integrity, confidentiality, authentication, and many more. However, many security techniques also exist to secure data. But all the existing techniques have some loopholes because of which data is not secure on the web. In the work, a reversible information embedding technique has been proposed. Secret information was taken in the form of text and covered as an image. Embedding capacity was improved because of text as secret data. Encryption is also combined with the steganography technique to improve the level of security. At the destination, the complete

secret data was retrieved efficiently with good visual quality [10]. Steganography techniques embed the confidential information in such a way that no one except the sender and receiver can detect it. Whereas, steganalysis techniques are applied to perceive the concealed secret message. In the work, both steganography and steganalysis techniques were studied. The analysis of these techniques was done based on various parameters [11]. After the literature review some of the challenges are listed as follows:

- The tradeoff between embedding capacity, visual quality, and robustness
- Do not resist image processing attacks and steganalysis techniques
- Existing techniques are not able to handle different file formats of cover file
- High complexity in terms of time and cost
- Text and audio cover files are not efficient to hide secret data

3. Research Design and Implementation

In the research work, we designed an image steganography technique using LSB. The technique works efficiently on image formats which include BMP, JPEG, TIFF, and PNG. Image files are present in many different formats and it is very difficult to find out which format is best. It depends on the type of application for which you want to use the image. JPEG is a standard format created in 1992. It is the most widely used lossy image compression method in multimedia images. In it retrieval of the image at the receiver end is difficult because of its lossy nature and the quality of the image is also sometimes degraded. It reduces the size of the input file resulting in the easy storing and forwards of the input image. JPEG images have their application in banking, streaming multimedia, digital cinema, internet telephony, medical, etc. PNG is again another standard image format. It is a lossless compression method used in processing and forwarding multimedia information. It is first created in 1996 and these types of images are mostly used on websites as high-quality images [12].

A PNG image takes more memory as compared to JPEG images. 24-Bits PNG images can efficiently store 16.8 million colors. It provides the best color tone to the images as compared to other formats. It has applications in many fields such as image editing; images carry layering

and web images. BMP is also known as bitmap, mapping of domain to bits. It stores images independently of the display of stored images. It can store images in the form of color and monochrome independently. It is most widely used in windows because of its structure. BMP images have a large size and it provides lossless compression. These files can carry fixed as well as variable structures. More than one version of the same file can exist in BMP images. TIFF is created in 1986 and is most widely used these days. It can store information and images in the same file. It also stores a header that defines the structure of images. Its header carries information about image compression, data arrangement, size, definition, etc. Because of its flexible nature, it has applications in photography, graphic designing, industry, image editing, word processing, etc. It can provide both lossy as well as lossless compression [3]. The encoding and decoding algorithm to hide and retrieve the secret data are given as follow.

3.1 *Algorithm Encoding*

Input: Cover Image, Secret Data

Output: Stego Image

Start: 1. Store image size in width and height
2. Store the pixel integral value of the image in the variable array
3. Count the number of pixels
4. Add "@r7D1" as the ending of the secret message
5. Convert message into binary form
6. Check if we have a sufficient number of pixels to store a secret message
   - 6.1 if they are insufficient stop and return an error message
   - 6.2 If they are a sufficient number of pixels
     - 6.2.1 Replace pixel value stored in the array by secret message least significant bit at a time
     - 6.2.2 Now form a stego image from pixel value in the array and save it

End

Same image in different formats is taken as cover files and secret information is taken in the form of text. The carrier image is converted in the form of an array of integer values. Secret text is converted into binary

form before its actual embedding. If the pixels in the secret image are sufficient to hide the secret text, then pixel values of the array are substituted by the pixels of the secret data. If the pixels in the cover image are not sufficient to embed secret text pixels, then the algorithm generates the error message. So, after embedding the secret message cover file is converted to a stego file.

3.2 *Algorithm Decoding*

Input: Stego Image

Output: Secret message

Start 1. Store the pixel integral value of the image in the variable array
2. Store stego image bits
3. Convert bits into characters and store them in a variable until no more bits are left or "@r7D1" is found at end of the message.
4. Check
   4.1 If "@r7D1" is at end of the message return the whole message except the last 5 characters
   4.2 Else return an error stating that no message was found

End

During the process of secret message decoding, the stego file is converted back into the form of an array of pixels. These pixels are then converted to bits and then to characters. The process is repeated until "@ r7D1" is not found. If the secret message is not retrieved properly then the algorithm will show the error message and the complete process need to carry out again.

4. Result Analysis and Discussion

We have taken 'Lena' as the cover image because of its wide use in image processing techniques. Lena is a nice mixture of color, illumination, and lighting conditions. We have taken secret text message of 5000 characters to embed in the same Lena cover image having different formats including TIFF, PNG, JPEG, and BMP. Implementation of the work is done in Python. We have chosen Python because of its widely used library files and popularity. For the analysis of the experimental results, we have

calculated PSNR, MSE, Entropy, SSIM, Histogram analysis, capacity, Concealing time, and Retrieval time. To validateresults, Lena is taken in different formats. Results are analyzed by imperceptibility, complexity and robustness of the stego file.

4.1 *Complexity Analysis*

Concealing capacity, embedding and extraction time as shown in Table 2 represent the complexity of the work. The size of the confidential message concealed is 5000 characters. The time reserved to embed and extract the secret message varies with the amount of secret data. The total time reserved to embed and extract the secret message is calculated to be less than 2 seconds for the image formats including BMP, TIFF, JPEG, and PNG which is very less time. There is little variation in the time taken with the change in the format of the input image. Also, no extra hardware is required to execute the technique so it is a cost-efficient technique.

4.2 *Robustness Analysis*

Robustness means how resistant is the steganography technique against image processing attacks or steganalysis tools [13]. For checking the robustness of the proposed work, we have used two steganalysis tools: StegDetect and StegExpose. Steganalysis tools try to expose the embedded secret message from the stego file. After steganalysis, it has been concluded that the proposed technique is robust means no secret message is detected by both the tools. The steganalysis tools are applied to each format of stego images. StegDetect is the steganalysis tool to detect the hidden secret message in images. It works well with JPEG images compared to other formats of images. It has a size of 2323 KB and is created in 2011. It used a 64-bit system and is user-friendly in windows. It also works with Ubuntu. In it C and C++ library generally used for artificial intelligence-based applications, OpenCV, and computer vision. It has generally no bugs and does not require any support. It is open-source software and can be installed from GitHub. From Figure 3 it has been concluded that the mentioned tool is not able to notice the secret data. After execution of code, the blank screen appears which means the proposed technique is robust against the steganalysis tool.

```
PS C:\Users\VIVAAN\Downloads\Steganography-master\Steganography-master\stego_lsb> python -i StegDetect.py
>>> show_lsb("stago_jpeg.png",1)
>>> show_lsb("stago_png.png",1)
>>> show_lsb("stago_bmp.bmp",1)
>>> show_lsb("stago_tif.tif",1)
>>>
```

Figure 3

Steganalysis through StegDetect

StegExpose does quantitative analysis of the input image to find its size. It is the part of MSc project at the School of Computing of the University of Kent, in Canterbury, UK. It is generally used to detect the LSB steganography technique in PNG and BMP images which are lossless. It analyses the images in bulk instead of single images. It provides a command line interface for the detection of secret messages. It is an open-source tool and works well in windows.

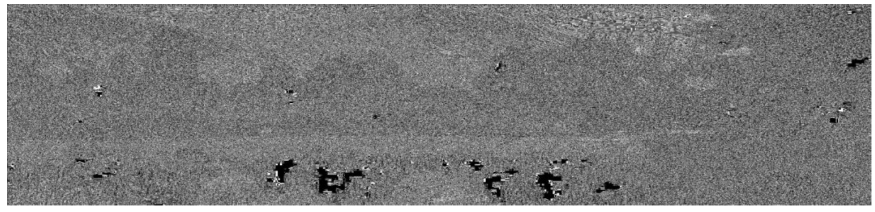


Figure 4

Steganalysis using StegExpose

Figure 4 shows the result of the StegExpose steganalysis tool. Again, StegExpose is also not able to perceive the concealed secret information. When the stego file is uploaded in the StegExpose tool the output appears in the form of a blank screen. The secret information hidden is in the form of the text so in case of detection of a secret message, the result must be in text form. From here it has been concluded that the proposed LSB technique is robust against steganalysis tools.

1.3 *Imperceptibility Analysis*

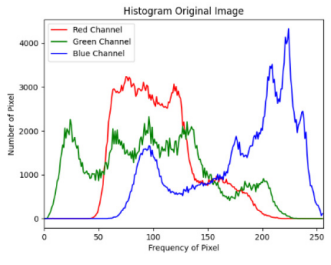
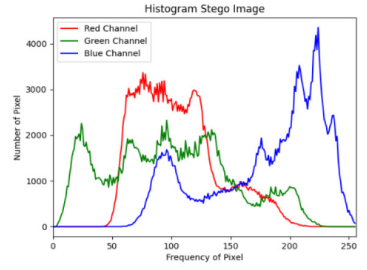
Imperceptibility stands for the visual excellence of the stego file. The higher the imperceptibility, the fewer the chances of exposure of secret message [14]. Imperceptibility can be checked with the help of evaluation parameters like PSNR, MSE, SSIM, Histogram analysis, Entropy, etc. Table 1 represents the analysis of the proposed work based on various evaluation parameters.

Table 1
Result Analysis

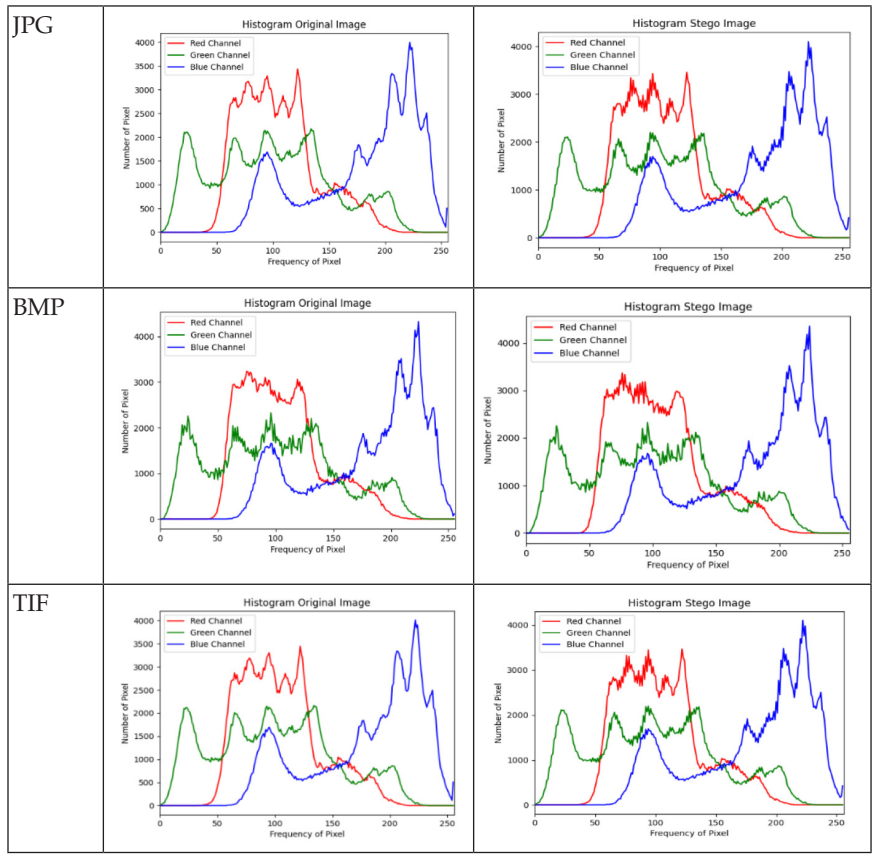
Image Format/ Parameters	PSNR	MSE	SSIM	Entropy of Original Image	Entropy of Stego Image	Concealing Time	Retrieval Time
BMP	57.11	0.156	0.9989	7.7502	7.7506	0.53	1.27
TIFF	56.19	0.159	0.9987	7.7548	7.7546	0.66	1.21
JPEG	56.55	0.160	0.9981	7.7558	7.7562	0.61	1.15
PNG	56.24	0.158	0.9984	7.7511	7.7515	0.55	1.22

There is little variation in the result with changes in the format of the image as revealed in the table also. The average PSNR value is calculated as 56 DB which represents high imperceptibility. The average error present among the original and stego file is calculated as approximately equal to 0.158 DB^2. The error is found to be negligible which can be ignored. The value of SSIM varies from 0 to 1 where 1 represents no variation in the structure of two images. For the proposed work SSIM is calculated as almost equal to 1 which means two files seem to be equal in structure. Entropy is the randomness between the original and the stego file. There is very less difference between the entropy of the two images which represents good quality of research work.

Table 2
Histograms for Original and Stego Frames

Image Format	Histogram of Original Cover Frame	Histogram of Stego Frame
PNG		

Contd...



The histogram represents the frequency distribution of the input image. As stego carry the hidden secret information so definitely there are some changes in the frequency distribution. We have calculated histograms for original and stego frames in the RGB color model. Small variations in histograms represent a good quality of work. We have drawn a histogram for BMP, Tiff, JPEG, and PNG image formats.

4.4 *Comparison of Proposed Work*

Comparison of the work is done with paper Kaur, H., & Kakkar, A. [5] as shown in Figure 5. JPEG, BMP, and PNG image formats are taken for comparison. In both, the papers LSB technique is used to hide secret information. For comparison, we have taken parameters such as PSNR, MSE, Processing time, and Payload. Although we worked on many other parameters also to analyze the work.

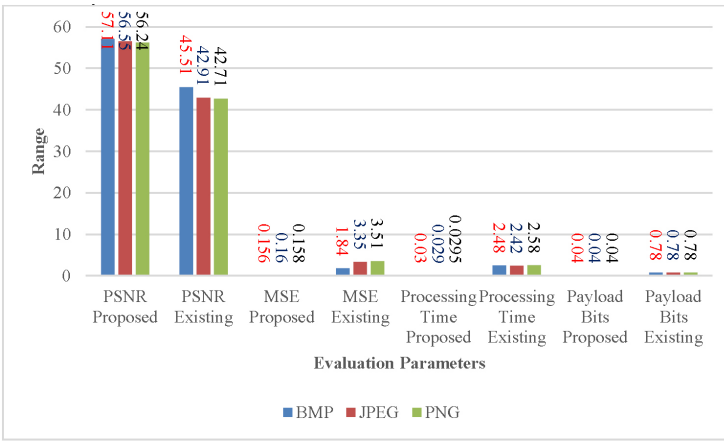


Figure 5

Comparative Analysis

PSNR for the proposed work is calculated to be approximately equal to 57 DB which is a good value compared to the existing work. MSE value is also found to be good for the work equated to the existing which is measured in DB^2. The total time to embed and retrieve the secret data is low in the case of the proposed work. The total time taken is represented in minutes in the comparison graph. For the proposed work it is calculated as less than 2 seconds and for the existing, it is found to be more than 2 minutes. In the existing work, the secret data embedded is very large compared to the proposed work. Embedding capacity is measured in MB. On embedding a large amount of data definitely, all other parameters also got affected such as PSNR, MSE, and processing time. So, we can conclude that on increasing the embedding capacity for the proposed work all other parameters degrade.

5. Conclusion and Future Scope

The proposed technique applies to all image formats including TIFF, BMP, PNG, and JPEG. We have embedded the same amount of text secret message that is KB in all four image formats. The analysis of the proposed work is done by checking complexity, imperceptibility and robustness. For imperceptibility, we calculated PSNR, MSE, SSIM, CC, and entropy. For all the formats imperceptibility is found to be satisfactory. Then to check robustness, we used two steganalysis tools: StegExpose and StegDetect. Both the tools fail to detect the hidden secret message. Time and cost

complexity is also found to be satisfactory. In future scope video in different formats can be taken as the cover file to hide the secret data. Video cover files can improve the embedding capacity because of their dynamic nature and large size.

Conflicts of Interest

The authors declare that they have no competing interests.

References

[1] El_Rahman, S. A., A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactor's confidential information. *Computers & Electrical Engineering*, 70, 380-399 (2018).

[2] Ansari, A. S., Mohammadi, M. S., & Parvez, M. T., A comparative study of recent steganography techniques for multiple image formats. *International Journal of Computer Network and Information Security*, 11(1), 11-25 (2019).

[3] Ansari, A. S., Mohammadi, M. S., & Parvez, M. T., A multiple-format steganography algorithm for color images. *IEEE Access*, 8, 83926-83939 (2020).

[4] Badr, S. M., Ismaial, G., & Khalil, A. H., A review on steganalysis techniques: from image format point of view. *International Journal of Computer Applications*, 102(4) (2014).

[5] Kaur, H., &Kakkar, A., Comparison of different image formats using LSB Steganography. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 97-101, IEEE (2017, September).

[6] Hashim, M. M., Rahim, M. S. M., Johi, F. A., Taha, M. S., & Hamad, H. S., Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. *International Journal of Engineering & Technology*, *7*(4), 3505-3514 (2018).

[7] Fridrich, J., Goljan, M., & Du, R., Detecting LSB steganography in color, and gray-scale images. *IEEE Multimedia*, 8(4), 22-28 (2001).

[8] Khaldi, A., Steganographic techniques classification according to image format. *International Annals of Science*, 8(1), 143-149 (2020).

[9] Anandpara, D., & Kothari, A., Working and comparative analysis of various spatial-based image steganography techniques. *International Journal of Computer Applications*, 113(12) (2015).

[10] Agham, V., &Pattewar, T., A novel approach toward separable reversible data hiding technique. In *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 771-775, IEEE (2014, February).

[11] Chandramouli, R., Kharrazi, M., & Memon, N., Image steganography and steganalysis: Concepts and practice. *In International Workshop on Digital Watermarking*, pp. 35-49, (2003, October) Springer, Berlin, Heidelberg.

[12] Pilania, U., Tanwar, R., Zamani, M., & Manaf, A. A., Framework for Video Steganography Using Integer Wavelet Transform and JPEG Compression. *Future Internet*, 14(9), 254 (2022).

[13] Pilania, U., Tanwar, R., Gupta, P., & Choudhury, T., A roadmap of steganography tools: conventional to modern. *Spatial Information Research*, 29(5), 761-774 (2021).

[14] Pilania, U., Stable High-Capacity Video Steganography in Wavelet Domain. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(7), 2142-2158 (2021).

Received February 2023